

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日  
Date of Application:

2002年 9月 4日

出 願 番 号  
Application Number:

特願2002-259190

[ ST.10/C ]:

[ JP2002-259190 ]

出 願 人  
Applicant(s):

株式会社日立製作所

2003年 2月14日

特 許 庁 長 官  
Commissioner,  
Japan Patent Office

太田信一郎

出証番号 出証特2003-3007962

【書類名】 特許願

【整理番号】 HI020539

【提出日】 平成14年 9月 4日

【あて先】 特許庁長官 殿

【国際特許分類】 G06F 1/26

【発明者】

【住所又は居所】 神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所 システム開発研究所内

【氏名】 大島 訓

【発明者】

【住所又は居所】 神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所 システム開発研究所内

【氏名】 佐藤 雅英

【特許出願人】

【識別番号】 000005108

【氏名又は名称】 株式会社日立製作所

【代理人】

【識別番号】 100071283

【弁理士】

【氏名又は名称】 一色 健輔

【選任した代理人】

【識別番号】 100084906

【弁理士】

【氏名又は名称】 原島 典孝

【選任した代理人】

【識別番号】 100098523

【弁理士】

【氏名又は名称】 黒川 恵

【選任した代理人】

【識別番号】 100112748

【弁理士】

【氏名又は名称】 吉田 浩二

【選任した代理人】

【識別番号】 100110009

【弁理士】

【氏名又は名称】 青木 康

【手数料の表示】

【予納台帳番号】 011785

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 セキュリティに関する情報を更新する方法、クライアント、サーバ、及び管理端末

【特許請求の範囲】

【請求項1】 クライアントとサーバとがネットワークを通じて接続され、前記サーバは、前記クライアントによって管理される記憶装置を備えるのであって、前記記憶装置にはセキュリティ情報が格納されており、

前記サーバにおける前記クライアントが管理する前記記憶装置に格納された前記セキュリティ情報を更新するステップを備えることを特徴とするセキュリティに関する情報を更新する方法。

【請求項2】 前記クライアントはローカルなディスク装置を有しないことを特徴とする請求項1に記載のセキュリティに関する情報を更新する方法。

【請求項3】 前記サーバは管理端末とネットワークを通じて接続され、前記セキュリティ情報を更新するステップでは、前記管理端末が、前記セキュリティ情報を更新することを特徴とする請求項1に記載のセキュリティに関する情報を更新する方法。

【請求項4】 前記サーバにおける前記クライアントが管理する前記記憶装置は、前記クライアントが使用するファイルを格納しており、

前記セキュリティ情報は、前記クライアントが使用する前記ファイルに関する属性であることを特徴とする請求項1に記載のセキュリティに関する情報を更新する方法。

【請求項5】 前記セキュリティ情報は、前記クライアントが使用する前記ファイルに対するアクセス制御情報であることを特徴とする請求項4に記載のセキュリティに関する情報を更新する方法。

【請求項6】 前記クライアントが前記セキュリティ情報を参照することを特徴とする請求項1に記載のセキュリティに関する情報を更新する方法。

【請求項7】 前記セキュリティ情報は、前記クライアントの使用をユーザに許可するための認証情報を含むことを特徴とする請求項6に記載のセキュリティに関する情報を更新する方法。

【請求項 8】 サーバにネットワークを通じて接続するクライアントであって、

前記クライアントが管理する記憶装置を前記サーバに備え、

前記記憶装置には、前記セキュリティ情報が格納されており、前記セキュリティ情報は更新され、

前記セキュリティ情報を参照することを特徴とするクライアント。

【請求項 9】 前記クライアントはローカルなディスク装置を有しないことを特徴とする請求項 8 に記載のクライアント。

【請求項 1 0】 前記サーバは管理端末とネットワークを通じて接続され、前記管理端末が、前記セキュリティ情報を更新することを特徴とする請求項 8 に記載のクライアント。

【請求項 1 1】 前記サーバにおける前記クライアントが管理する前記記憶装置は、前記クライアントが使用するファイルを格納しており、

前記セキュリティ情報は、前記クライアントが使用する前記ファイルに関する属性であることを特徴とする請求項 8 に記載のクライアント。

【請求項 1 2】 前記セキュリティ情報は、前記クライアントが使用する前記ファイルに対するアクセス制御情報であることを特徴とする請求項 1 1 に記載のクライアント。

【請求項 1 3】 前記セキュリティ情報は、前記クライアントの使用をユーザに許可するための認証情報を含むことを特徴とする請求項 8 に記載のクライアント。

【請求項 1 4】 クライアントとネットワークを通じて接続されるサーバであって、

前記クライアントによって管理される記憶装置を備え、

前記記憶装置には、前記セキュリティ情報が格納され、前記セキュリティ情報は更新されることを特徴とするサーバ。

【請求項 1 5】 前記クライアントはローカルなディスク装置を有しないことを特徴とする請求項 1 4 に記載のサーバ。

【請求項 1 6】 前記サーバは管理端末とネットワークを通じて接続され、

前記管理端末が、前記セキュリティ情報を更新することを特徴とする請求項 1 4 に記載のサーバ。

【請求項 1 7】 前記サーバにおける前記クライアントが管理する前記記憶装置は、前記クライアントが使用するファイルを格納しており、

前記セキュリティ情報は、前記クライアントが使用する前記ファイルに関する属性であることを特徴とする請求項 1 4 に記載のサーバ。

【請求項 1 8】 前記セキュリティ情報は、前記クライアントが使用する前記ファイルに対するアクセス制御情報であることを特徴とする請求項 1 7 に記載のサーバ。

【請求項 1 9】 前記セキュリティ情報は、前記クライアントにより参照されることを特徴とする請求項 1 4 に記載のサーバ。

【請求項 2 0】 前記セキュリティ情報は、前記クライアントの使用をユーザに許可するための認証情報を含むことを特徴とする請求項 1 9 に記載のサーバ。

【請求項 2 1】 クライアントによって管理される記憶装置を備えたサーバとネットワークを通じて接続される管理端末であって、

前記サーバの前記記憶装置には、前記セキュリティ情報が格納されており、前記セキュリティ情報を更新することを特徴とする管理端末。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

この発明は、セキュリティに関する情報を更新する方法、クライアント、サーバ、及び管理端末に関する。

【0 0 0 2】

【従来の技術】

ネットワークを介してサーバに接続されるクライアントは、図 7 に示すように、CPU、メモリ、ネットワークインタフェース、及びハードディスク装置で構成されるストレージ（ローカルなディスク装置）を備えている。メモリには、OS (Operating System)、セキュリティソフトウェア及びアプリケーションプロ

グラムが展開される。ストレージには各種ファイルが記憶されている。これら各種ファイルとしては、OSを構成するファイル群やポリシファイル群、及び、その他ファイル群である。その他ファイル群としては、セキュリティソフトウェア、アプリケーションプログラム、データファイル（適宜、単にファイルと称する）、及びファイルシステムが含まれる。このファイルシステムには、各ファイルの属性やファイルアロケーションテーブル等、様々なファイルの管理情報が記述されている（例えば、非特許文献1参照）。

#### 【0003】

一般的なOSの制御の下では、図8に示すように、アプリケーションプログラムがファイルに対してアクセスを要求すると（S10）、ファイルアクセス制御機能によりファイルシステムが参照され、アクセスの可否が判定される（S20）。この判定で許可されると、アプリケーションプログラムはドライバによりファイルにアクセスできる（S30→S40）。また、アプリケーションプログラムがアクセスするファイルは、ネットワークを介して接続されるサーバ側のファイルも含む。すなわち、ネットワークドライバ及びネットワークカードにより、ネットワークを介して接続されるサーバ側のファイルにアクセスする（S50→S60→S70）。

#### 【0004】

このストレージに格納されるファイルシステムの内容としては、例えば、ファイル属性（図2参照、例えば、非特許文献2参照）、アロケーションテーブル（図3参照）、及びクラスタ（図4参照）がある。図2のファイル属性に示すように、各ファイルについて、ファイル名やパス名をはじめ、所有者やグループ名等の属性が対応づけられている。特に、所有者やグループ、及び外部といったユーザからの各ファイルへのアクセスに関し、読み出し（図中「読」）や書き込み（図中「書」）及び実行といった各項目を設けている。そして、これら各項目について、許可（図中「可」）や不許可（図中「不」）といったアクセス権に関する属性が対応づけられている。

#### 【0005】

そして、図7に示すセキュリティソフトウェアは、OSに追加するソフトウェア

アであり、前述したアクセス制御機能を強化する。このセキュリティソフトウェアは、ポリシファイルに記述されたアクセス制御情報に基づき、よりセキュリティを高める緻密なアクセス制御を行う。このポリシファイルには、ファイルに対するアクセスを許可する条件として、ユーザやアプリケーション及び時間帯等の詳細な属性が特定されている。

【0006】

また、このポリシファイルには、ウイルスパターンファイルや、シグネチャファイルも含まれる。ウイルスパターンファイルは、アンチウイルスソフトと称されるウイルス対策用ソフトウェアに用いられる。シグネチャファイルは、ホスト型侵入検知システムと称されるネットワーク攻撃対策用ソフトウェアに用いられる。アンチウイルスソフトは、コンピュータウイルスの特徴を示すパターンに基づき、ファイルのオープン時または一定期間毎に、ファイルに対するコンピュータウイルスの感染の有無を検査し、必要な処置を適宜に講じる。ホスト型侵入検知システムは、シグネチャと呼ばれるネットワークパケットを識別し、ネットワークを通じた攻撃を検知したり、実行中のアプリケーションプログラムが出力したログファイル等を監視し、攻撃を検知する。

【0007】

ここで、ポリシ（セキュリティポリシ）とは、コンピュータの使用に関する制限を総称したセキュリティ情報である。つまり、ポリシとは、特定のアプリケーションの実行を禁止したり、設定変更を防止するための情報だけでなく、各種ソフトウェアも含む。

【0008】

次に、ネットワーク環境下におけるポリシファイルの更新について説明する。図9に示すように、まず、電源を投入してクライアントを起動させる（S100）と、そのOSが起動する（S110）。起動したOSの制御により、ネットワーク接続や各種ソフトウェアによるサービスが起動し（S120）、ネットワークを介したデータの授受が可能となる。そして、クライアントは、セキュリティソフトウェアの実行によりポリシファイルの更新機能が起動し（S130）、ネットワークを介して管理端末から、前述したポリシファイルの更新を受ける。す



なわち、クライアントは、管理端末からポリシファイルの最新バージョンを受信する（S130）。そして、クライアントは、ユーザの操作入力に応じた各種の処理が実行可能となる（S140）。

【0009】

【非特許文献1】

村瀬康治著「入門MS-DOS 改訂新版」株式会社アスキー出版、1991年8月11日p. 63-64

【0010】

【非特許文献2】

村瀬康治著「入門MS-DOS 改訂新版」株式会社アスキー出版、1991年8月11日p. 131-132

【0011】

【発明が解決しようとする課題】

前述した従来技術にあつては、クライアントに付帯するストレージにポリシファイルが格納されている。このため、クライアントの動作が停止中では、当然ながら、ポリシファイルを更新することができない。このため、ポリシファイルを更新するまでの間、アクセス制御やウイルス対策等を最新の状態で行うことができない。

【0012】

また、図9のフローチャートで示したように、起動後にクライアントのポリシファイルが更新されるため、起動してからアップデートされるまでの間、古いバージョンのセキュリティ情報で運用されることになる。この間、アクセス制御やウイルス対策等を最新の状態で行うことができない。特に、ネットワーク感染型のウイルスは、ネットワークに接続されている機器に対して攻撃する。このため、起動してからアップデートされるまでの間、クライアントは常時攻撃を受けうる無防備な状態となってしまう。

【0013】

さらに、ポリシの更新作業に関し、複数あるクライアントそれぞれについて、ポリシの更新作業を実施しなければならず、各クライアントすべての管理負担が

膨大となる。

【 0 0 1 4 】

【課題を解決するための手段】

本発明が提供する主たる技術では、クライアントとサーバとがネットワークを通じて接続され、前記サーバは、前記クライアントによって管理される記憶装置を備えるのであって、前記記憶装置にはセキュリティ情報が格納されており、前記サーバにおける前記クライアントが管理する前記記憶装置に格納された前記セキュリティ情報を更新する。

本発明の他の特徴については、本明細書及び添付図面の記載により明らかにする。

【 0 0 1 5 】

【発明の実施の形態】

===== 発明の概要 =====

本明細書及び添付図面の記載により、少なくとも次の事項が明らかとなる。

本実施の形態に係る、セキュリティに関する情報を更新する方法では、クライアントとサーバとがネットワークを通じて接続され、前記サーバは、前記クライアントによって管理される記憶装置を備えるのであって、前記記憶装置にはセキュリティ情報が格納されており、

前記サーバにおける前記クライアントが管理する前記記憶装置に格納された前記セキュリティ情報を更新するステップを備える。

前記クライアントはローカルなディスク装置を有しないこととできる。

前記サーバは管理端末とネットワークを通じて接続され、前記セキュリティ情報を更新するステップでは、前記管理端末が、前記セキュリティ情報を更新することとできる。

前記サーバにおける前記クライアントが管理する前記記憶装置は、前記クライアントが使用するファイルを格納しており、前記セキュリティ情報は、前記クライアントが使用する前記ファイルに関する属性であることとできる。

前記セキュリティ情報は、前記クライアントが使用する前記ファイルに対するアクセス制御情報であることとできる。

前記クライアントが前記セキュリティ情報を参照することとできる。

前記セキュリティ情報は、前記クライアントの使用をユーザに許可するための認証情報を含むこととできる。

【0016】

本実施の形態に係るクライアントでは、サーバにネットワークを通じて接続するのであって、前記クライアントが管理する記憶装置を前記サーバに備え、前記記憶装置には、前記セキュリティ情報が格納されており、前記セキュリティ情報は更新され、前記セキュリティ情報を参照する。

前記クライアントはローカルなディスク装置を有しないこととできる。

前記サーバは管理端末とネットワークを通じて接続され、前記管理端末が、前記セキュリティ情報を更新することとできる。

前記サーバにおける前記クライアントが管理する前記記憶装置は、前記クライアントが使用するファイルを格納しており、前記セキュリティ情報は、前記クライアントが使用する前記ファイルに関する属性であることとできる。

前記セキュリティ情報は、前記クライアントが使用する前記ファイルに対するアクセス制御情報であることとできる。

前記セキュリティ情報は、前記クライアントの使用をユーザに許可するための認証情報を含むこととできる。

【0017】

本実施の形態に係るサーバでは、クライアントとネットワークを通じて接続されるのであって、前記クライアントによって管理される記憶装置を備え、前記記憶装置には、前記セキュリティ情報が格納され、前記セキュリティ情報は更新される。

前記クライアントはローカルなディスク装置を有しないこととできる。

前記サーバは管理端末とネットワークを通じて接続され、前記管理端末が、前記セキュリティ情報を更新することとできる。

前記サーバにおける前記クライアントが管理する前記記憶装置は、前記クライアントが使用するファイルを格納しており、前記セキュリティ情報は、前記クライアントが使用する前記ファイルに関する属性であることとできる。

前記セキュリティ情報は、前記クライアントが使用する前記ファイルに対するアクセス制御情報であることとできる。

前記セキュリティ情報は、前記クライアントにより、参照されることとできる。

前記セキュリティ情報は、前記クライアントの使用をユーザに許可するための認証情報を含むこととできる。

#### 【 0 0 1 8 】

本実施の形態に係る管理端末では、クライアントによって管理される記憶装置を備えたサーバとネットワークを通じて接続されるのであって、前記サーバの前記記憶装置には前記セキュリティ情報が格納されており、前記セキュリティ情報を更新する。

#### 【 0 0 1 9 】

===== 実施例 =====

クライアントは、ローカルのハードディスク装置を備えない、いわゆるディスクレスのコンピュータで構成される。本実施例では、このクライアントをディスクレスクライアントと称する。

#### 【 0 0 2 0 】

図 1 に示すように、一又は複数台のディスクレスクライアント 1 0 0 がネットワークを介してストレージサーバと称するサーバ 2 0 0 に接続する。このサーバ 2 0 0 には、ネットワークを介して管理端末 3 0 0（図中では管理用計算機）が接続される。なお、この管理端末 3 0 0 の機能をサーバ 2 0 0 が備えることで、管理端末 3 0 0 を省略してもよい。

#### 【 0 0 2 1 】

ディスクレスクライアント 1 0 0 は、従来同様、CPU 1 1 0、メモリ 1 2 0 及びネットワークインタフェース 1 3 0 を装備している。メモリ 1 2 0 には、OS 1 2 1、セキュリティソフトウェア 1 2 2、アプリケーションプログラム 1 2 3、及びネットワークストレージドライバ 1 2 4 がサーバ 2 0 0 から読み出されて展開される。また、ディスクレスクライアント 1 0 0 は、その記憶装置の機能をディスクイメージ 2 2 0 としてサーバ 2 0 0 に持たせている。

すなわち、ディスクレスクライアント100は、ローカルなディスク装置を有さず、サーバ200のハードディスク装置（ストレージ、記憶装置）がマウントされている。ディスクレスクライアント100のネットワークストレージドライバ124が、ネットワーク経由でマウントされたサーバ200のディスクを制御する。

#### 【0022】

サーバ200は、ネットワークインタフェース210及びCPU220を備えるとともに、各ディスクレスクライアント100が管理するハードディスク装置を多数備える。このサーバ200は、例えばRAID（Redundant Array of Inexpensive Disks）方式で運用してもよい。ハードディスク装置には、ディスクレスクライアント100が使用するディスクイメージ230が格納される。このディスクイメージ230は、各ディスクレスクライアント100毎に存在する。このディスクイメージ230とは、前述した図7に示す従来のクライアントのストレージ（ハードディスク装置）に格納されたものと同じファイル群である。

すなわち、ディスクレスクライアント100が使用するディスクイメージ230は、OSの構成に関するOS構成ファイル群231、ポリシーファイル群232及びその他のファイル群233である。これらファイル群231乃至233には、前述した従来の技術と同様のセキュリティ情報が含まれる。

すなわち、ポリシーファイル群232は、前述した、アクセス制御情報、ウィルスパターンファイル、及びシグネチャファイル等で構成される。その他のファイル群233は、セキュリティソフトウェア122、アプリケーションプログラム123、及びソフトウェアやプログラムが使用するデータファイル、ネットワークストレージドライバ124を含む。加えて、その他のファイル群233には、ファイルの属性やファイルアロケーションテーブル等、図2乃至図4に示すように様々なファイルの管理情報がファイルシステムとして含まれる。

#### 【0023】

管理端末300は、CPU310、メモリ330、ネットワークインタフェース320、及びハードディスク装置で構成されるストレージ340を備えている。メモリ330には、OS331、管理用ソフトウェア332及びアプリケーション

ョンプログラム333が展開される。ストレージ340には、OS、管理ソフトウェア及びアプリケーションプログラム及びデータファイル等、各種ファイル群341乃至343が格納されている。管理用ソフトウェア332が管理ソフトウェアファイル群342を用いて、サーバ200のディスクイメージ230における各種ファイル群341乃至343の内容、すなわち、セキュリティ情報を更新して最新のバージョンとする。

#### 【0024】

具体的なポリシーのアップデート手順を図5に示す。図1に示すように、従来と異なり、ディスクレスクライアント100が使用するポリシーは、サーバ200が保持する各種ファイル群231乃至233に含まれる。そして、随時、サーバ200がポリシーのアップデート機能を起動し（S200）、管理端末300から適宜各種ファイル群231乃至233の最新版を受け取り、ポリシーのアップデートを完了する（S210）。このことで、サーバ200が接続するネットワーク全体において、ファイルの属性やユーザIDをはじめ、各種ウイルス対策等のポリシーのアップデートが行われる。このことで、不正アクセスやウイルスの侵入や攻撃等に対し、最新のセキュリティが確保される。

#### 【0025】

このポリシーのアップデートの完了後に、ディスクレスクライアント100が起動する（S220）。詳しくは、ディスクレスクライアント100が電源投入されるとIPL（Initial Program Loader）が起動される。IPLの作用によりネットワークを通じてサーバ20のディスクイメージ230から基本OSが呼び出され、ディスクレスクライアント100のメモリ120に基本OSが展開される。展開された基本OSが動作を開始（S230）することにより、ディスクレスクライアント100はコンピュータとしての動作を開始する。

#### 【0026】

起動したOSの制御により、ディスクレスクライアント100は、ネットワーク接続や各種ソフトウェアによるサービスが起動し（S240）、ネットワークを介したデータの授受が可能となる。動作を開始したディスクレスクライアント100は、ユーザのID（ユーザ名）やパスワード等の認証情報の入力を受け付

けると、サーバ200のディスクイメージ230内のファイル群231、232内に登録された認証情報と照合する。照合の結果、グループID（グループ名）も含めた認証情報の正当性が確認されると、ユーザによるクライアントの使用を可能とする。

## 【0027】

ディスクレスクライアント100でアプリケーションプログラムが動作する場合において、セキュリティソフトウェア122によるセキュリティを高める追加のアクセス制御について説明する。セキュリティソフトウェア122は、前述したアクセス制御機能を強化すべく、OSに追加するソフトウェアである。このセキュリティソフトウェア122は、ポリシーファイルに記述されたアクセス制御情報に基づき、よりセキュリティを高める緻密なアクセス制御を行う。このポリシーファイルには、アプリケーションプログラム等が使用するファイルに対するアクセスを許可する条件として、ユーザやアプリケーション及び時間帯等の詳細な属性が特定されている。

## 【0028】

すなわち、図6のフローチャートに示すように、OSの制御の下では、図1のアプリケーションプログラム123が、サーバ200のディスクイメージ230内のファイルに対してアクセスを要求すると（S310）、セキュリティソフトウェア122による追加のファイルアクセス制御が機能する（S311）。このファイルアクセス制御により、サーバ200のディスクイメージ230内のポリシーファイル232を参照し、アクセスが要求されたファイルについて、そのポリシーを確認する（S312）。このポリシーとしては、各ファイルに関し、その属性、アクセスを許可するユーザIDやアプリケーションを特定する情報である。このポリシーの確認の結果、アプリケーションによるファイルアクセスが許可されると、次にOSによるファイルアクセス制御が機能する。このOSのファイルアクセス制御により、アクセスが要求されたファイルについて、そのファイルシステムを参照し、図4に示すファイル属性を確認する（S313）。この確認の結果、ユーザIDが一致する等でアクセスが許可されると、ネットワークストレージドライバ124がネットワークインタフェース130を介し、サーバ200のデ

ィスクイメージ230内のファイルにアクセスする（S314→S315→S316）。

【0029】

以上、本発明の実施の形態について、その実施の形態に基づき具体的に説明したが、これに限定されるものではなく、その要旨を逸脱しない範囲で種々変更可能である。

【0030】

本発明の実施の形態にあつては次の効果を奏する。

ディスクレスのクライアントが管理して使用するディスクは、ネットワーク上のサーバにマウントされている。加えて、このサーバにマウントされたディスクには、ポリシ（セキュリティポリシ）やファイルを含むクライアントのディスクイメージが格納されている。そして、このディスクイメージにおけるポリシの更新については、管理端末が行う。

【0031】

このため、クライアントの動作停止の有無に関わらず、随時、ポリシ（セキュリティ情報）を更新することができる。したがって、停止中のクライアントが起動した時点では、既にポリシの更新が完了している。このため、クライアントは常時更新されたポリシに則って運用される。

【0032】

複数のクライアントが一つのサーバにディスクをマウントする場合でも、サーバのポリシを更新するだけで済む。例えば、管理端末を介してサーバのポリシを更新する。すなわち、従来のように、各クライアントそれぞれについて、ポリシの更新作業を実施する必要がなく、各クライアントの管理負担を大幅に軽減することができる。

【0033】

【発明の効果】

クライアントが動作停止中でも、セキュリティ情報を更新することができる。

【図面の簡単な説明】

【図1】 本発明に係る一実施例を示すシステムブロック図である。



【図 2】 本発明に係る一実施例におけるファイル属性を示す図表である。

【図 3】 本発明に係る一実施例におけるアロケーションテーブルを示す図表である。

【図 4】 本発明に係る一実施例におけるクラスタの構造を示す図表である。

【図 5】 本発明に係る一実施例におけるポリシーのアップデート手順を示すフローチャートである。

【図 6】 本発明に係る一実施例におけるファイルの追加的なアクセス制御を示すフローチャートである。

【図 7】 本発明に係る一実施例におけるクライアントの構成を示すブロック図である。

【図 8】 従来のクライアントによるファイルに対するアクセスの制御を示すフローチャートである。

【図 9】 従来のクライアントによるポリシーファイルの更新を示すフローチャートである。

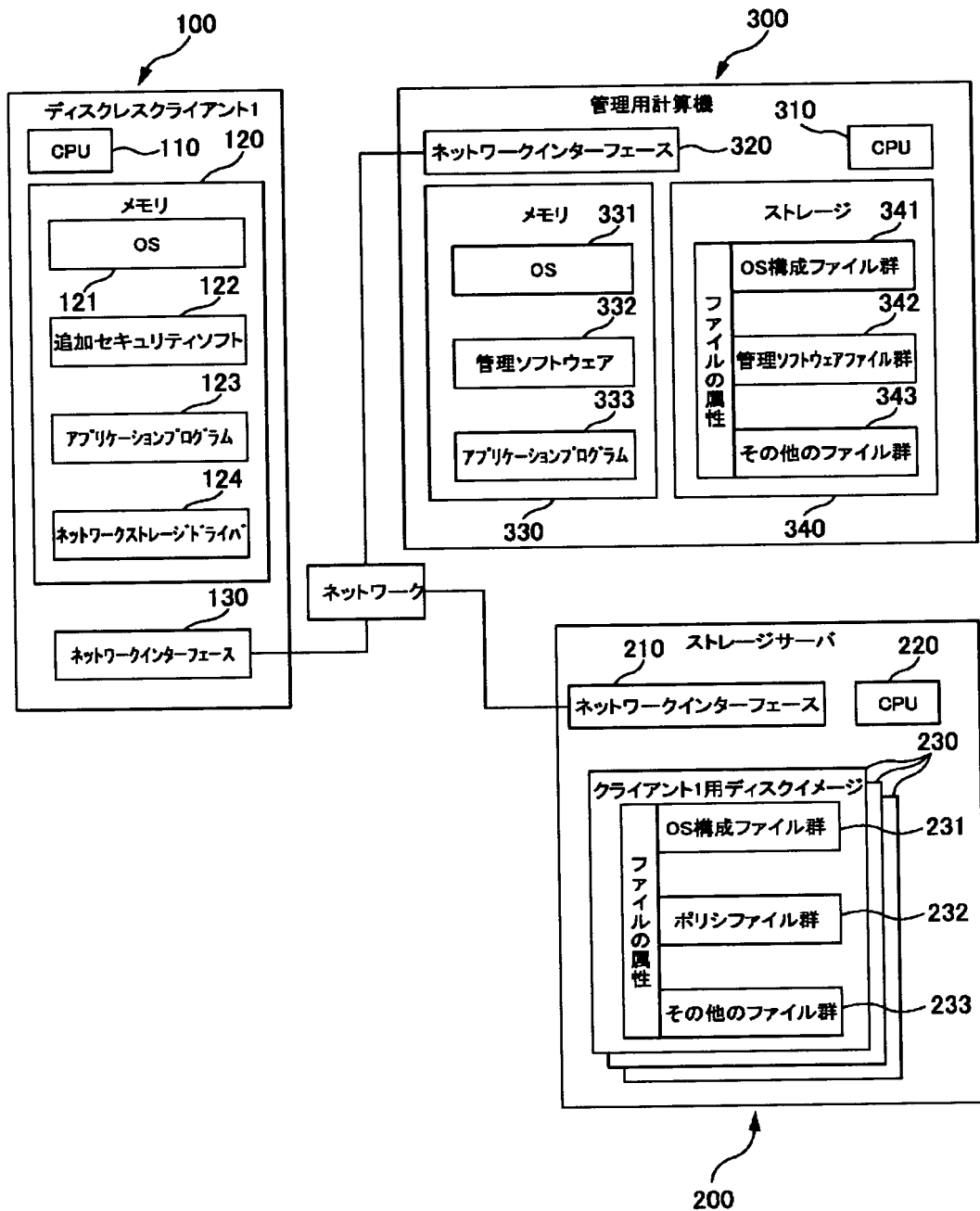
#### 【符号の説明】

- 1 0 0 ディスクレスクライアント
- 1 1 0 CPU
- 1 2 0 メモリ
- 1 2 1 OS
- 1 2 2 セキュリティソフトウェア
- 1 2 3 アプリケーションプログラム
- 1 2 4 ネットワークストレージドライバ
- 1 3 0 ネットワークインタフェース
- 2 0 0 サーバ
- 2 1 0 ネットワークインタフェース
- 2 2 0 CPU
- 2 3 0 ディスクイメージ
- 2 3 1 OS構成ファイル群

- 2 3 2 ポリシファイル群
- 2 3 3 その他のファイル群
- 3 0 0 管理端末
- 3 1 0 C P U
- 3 2 0 ネットワークインタフェース
- 3 3 0 メモリ
- 3 3 1 O S
- 3 3 2 管理用ソフトウェア
- 3 3 3 アプリケーションプログラム
- 3 4 0 ストレージ
- 3 4 1 O S 構成ファイル群
- 3 4 2 管理ソフトウェアファイル群
- 3 4 3 その他のファイル群

【書類名】 図面

【図 1】



【図 2】

ファイル属性

ファイル名	パス名	日付			所有者名	グループ名	所有者			グループ			外部			AT
		作成	変更	参照			読	書	実行	読	書	実行	読	書	実行	
test.txt	%tmp%	2000/2/3	2001/3/4	2001/4/5	usera	groupa	可	可	否	可	否	否	可	否	否	15
foo.doc	%sys%	2002/1/1	2002/1/1	2002/5/6	root	root	可	否	否	否	否	否	否	否	否	23
bar.exe	%bin%	2000/2/3	2000/2/3	2002/5/6	daemon	daemon	可	可	可	可	否	可	可	否	可	48
...																

【図 3】

アロケーションテーブル(4~8バイト/マス)

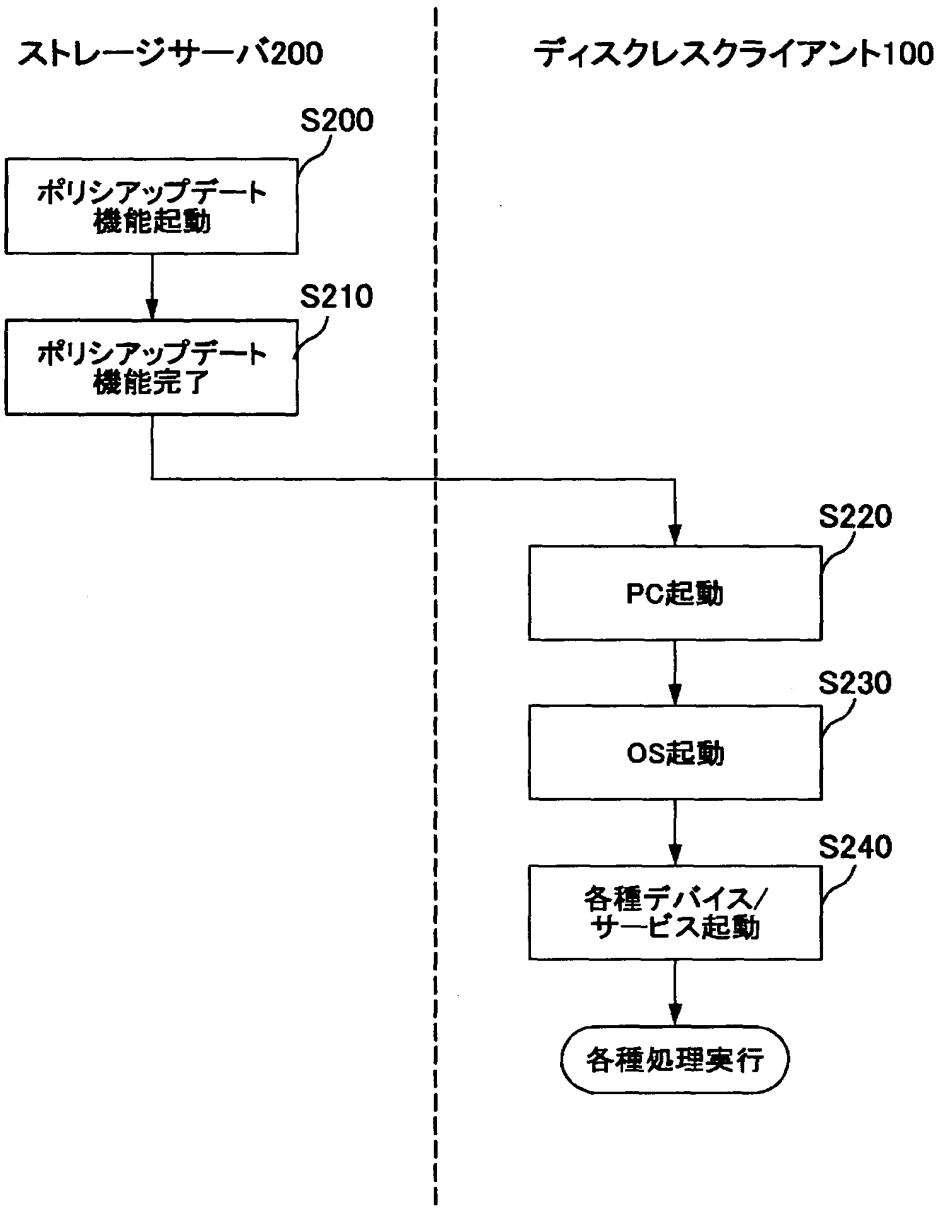
	0	1	2	3	4	5	6	7	8	9
0			5			8			63	
10						16	17	18	19	20
20	0			24	25	30				
30	31	32	33	0						
40									2	
50										
60				67				0		
...										

【図 4】

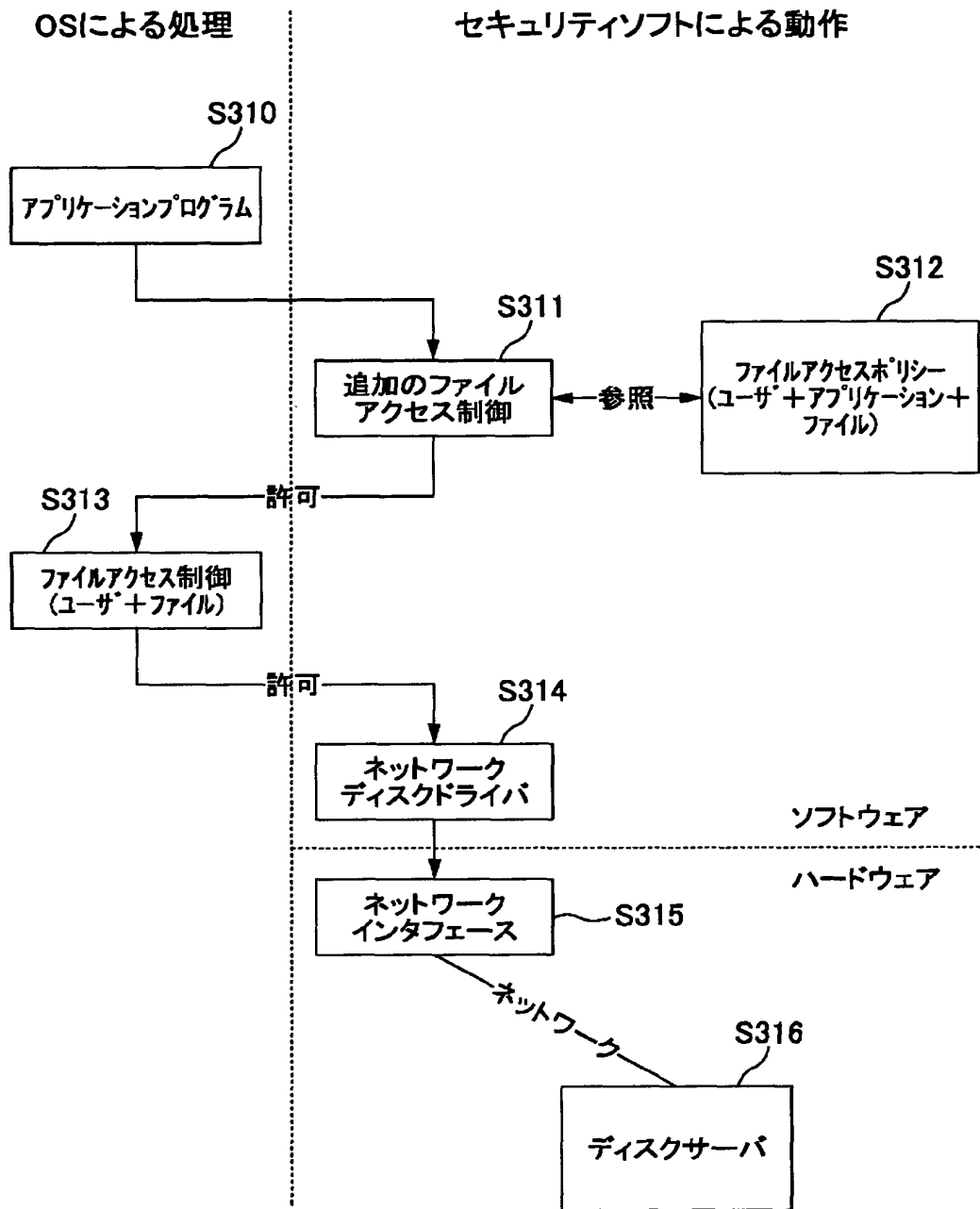
クラスタ(4~32バイト/マス)

	0	1	2	3	4	5	6	7	8	9
0			*			*			*	
10						*	*	*	*	*
20	*			*	*	*				
30	*	*	*	*						
40									*	
50										
60				*				*		
...										

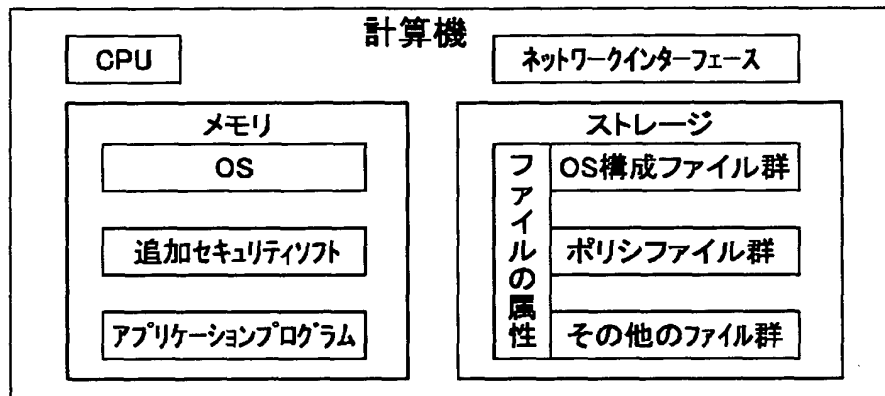
【図 5】



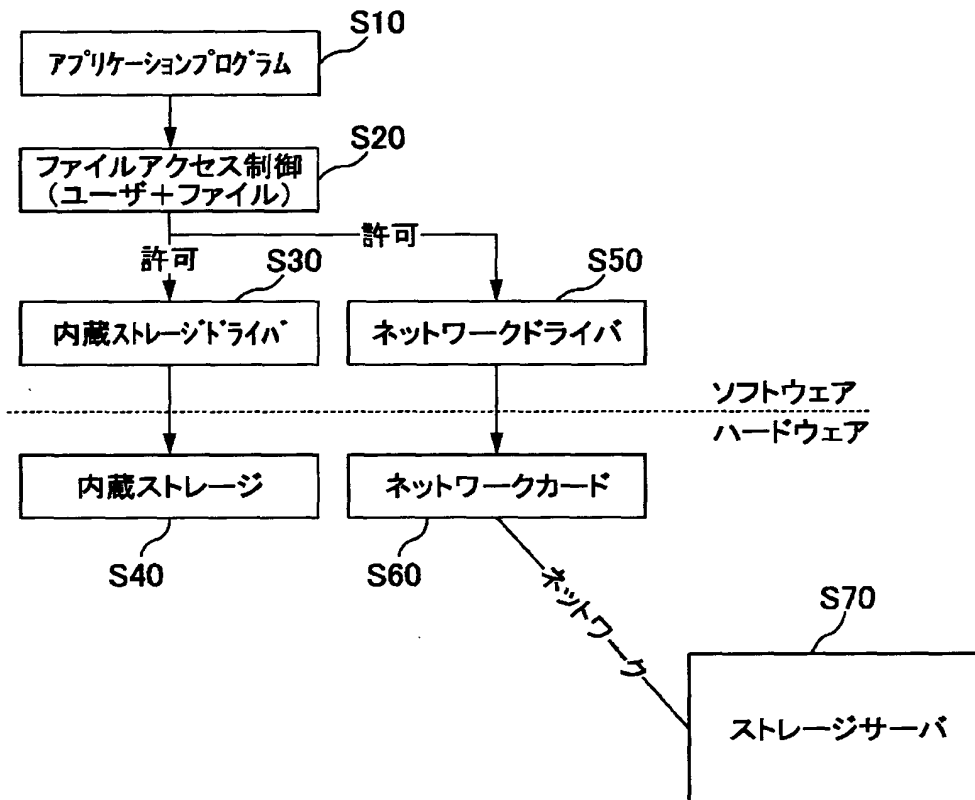
【図 6】



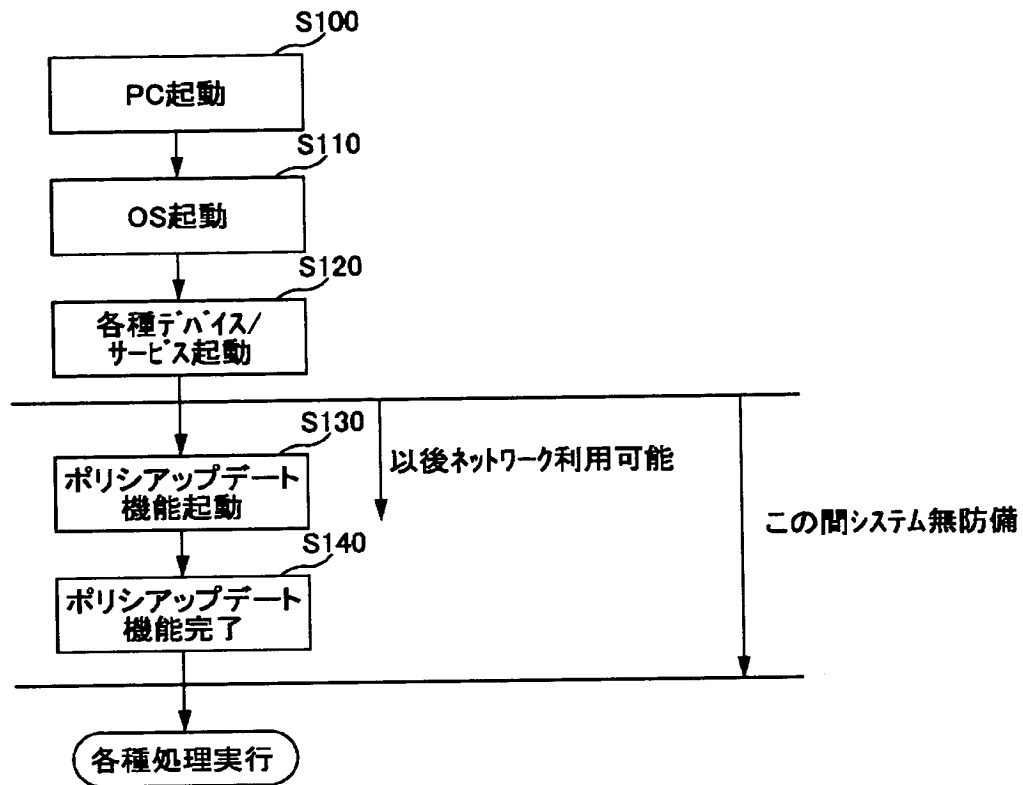
【図 7】



【図 8】



【図 9】





【書類名】 要約書

【要約】

【解決手段】 クライアントとサーバとがネットワークを通じて接続され、前記サーバは、前記クライアントによって管理される記憶装置を備えるのであって、前記記憶装置にはセキュリティ情報が格納されており、前記サーバにおける前記クライアントが管理する前記記憶装置に格納された前記セキュリティ情報を更新する。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000005108]

1. 変更年月日 1990年 8月31日

・ [変更理由] 新規登録

住 所 東京都千代田区神田駿河台4丁目6番地

氏 名 株式会社日立製作所